(6)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312221
(43)Date of publication of application : 25.10.2002

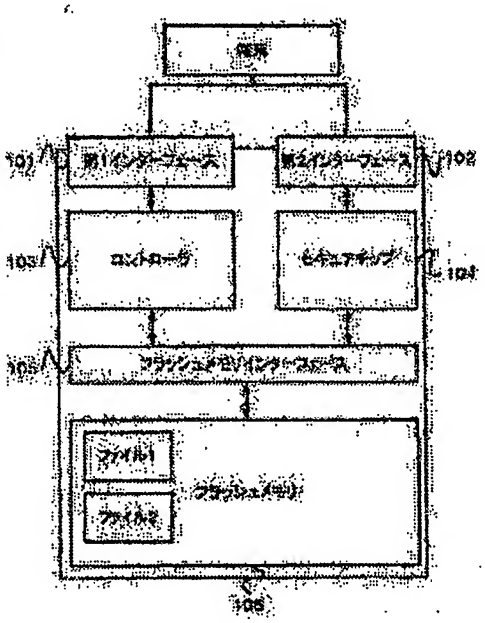
(51)Int.Cl. G06F 12/00
G06F 12/14
G06K 19/073

(21)Application number : 2001-118507
(22)Date of filing : 17.04.2001

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : TAKAGI YOSHIHIKO
NAKANISHI YOSHIAKI
SASAKI OSAMU

(54) MEMORY DEVICE WITH ACCESS CONTROL FUNCTION AND FAILE ACCESS CONTROL PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a high protective property against wrong deletion and dishonest alteration of data in a memory device to write and read data.
SOLUTION: The memory device is provided with a controller 103 and a secure chip 104. A file, which is set so that its attribute cannot be changed when the secure chip 104 inputs 0 for a flag for determining whether the attribute of the access attribute peculiar to the file can be changed or not, cannot change the access attribute peculiar to the file by obtaining access through the controller 103. In a file, which is made through the controller 103, the flag for determining whether the attribute can be changed or not always becomes 1, making it possible to change the attribute freely. This constitution makes it possible to perform access control according to the degree of importance. In addition, in obtaining access through the secure chip 104, by applying access attribute according to conditions, a file to which access can be obtained only under a specific condition can be stored.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－312221
（P2002－312221A）
(43)公開日　平成14年10月25日(2002.10.25)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
G06F	12/00	537	G06F	12/00	537H 5B017
		542			542J 5B035
	12/14	310		12/14	310K 5B082
G06K	19/073		G06K	19/00	P

審査請求　未請求　請求項の数14　ＯＬ　（全 12 頁）

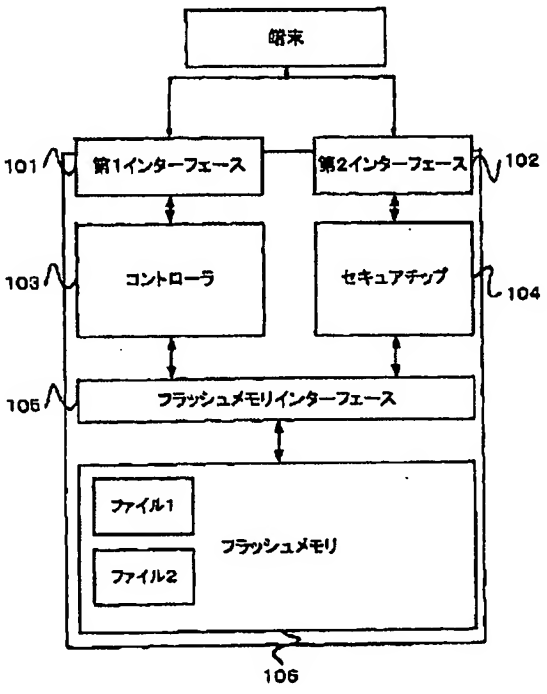
(21)出願番号　特願2001－118507(P2001－118507)
(22)出願日　平成13年４月17日(2001.4.17)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　高木　佳彦
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　中西　良明
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100082692
弁理士　蔵合　正博　（外１名）

最終頁に続く

(54)【発明の名称】　アクセス制御機能付き記憶装置、及びファイル・アクセス制御プログラム

(57)【要約】
【課題】　データの書き込み、読み出しを行う記憶装置において、データの不正な削除、改ざんに対して高い防御性を実現することを目的とする。
【解決手段】　記憶装置にコントローラ１０３とセキュアチップ１０４を設け、セキュアチップ１０４がファイル固有のアクセス属性の属性変更可否フラグを０にすることによって属性変更不可に設定したファイルは、コントローラ１０３経由のアクセスではファイル固有のアクセス属性を変更できない。一方コントローラ１０３経由で作成したファイルは属性変更可否フラグは常に１となり、属性変更は自由である。これにより、ファイルの重要度に応じたアクセス制御を行うことができる。さらにセキュアチップ１０４経由のアクセスでは条件に応じたアクセス属性を適用することで、特定の条件下でのみアクセス可能なファイルを格納することができる。



1

【特許請求の範囲】

【請求項１】　ファイルと前記ファイルに固有のアクセス属性である第１の属性情報を格納する記憶手段と、
前記第１の属性情報を参照して前記ファイルに対するアクセス制御を行う第１のアクセス制御手段と、
前記記憶手段内部のファイルに対する条件に応じたアクセス属性を記述した第２の属性情報を格納する手段と、
前記第２の属性情報を参照して前記ファイルに対するアクセス制御を行う第２のアクセス制御手段と、を備えたアクセス制御機能付き記憶装置。

【請求項２】　第２のアクセス制御手段が、
前記第２のアクセス制御手段内部で実行するプログラムを記憶する手段と、前記プログラムの選択実行手段と、
第２の属性情報を参照して前記プログラムによるファイルに対するアクセスの可否を判定する属性参照手段とを有し、
前記第２の属性情報は、
ファイルを一意に示す第１の参照情報と、
前記ファイルに対してアクセスし得る１つ以上のプログラムをそれぞれ一意に示す第２の参照情報と、
前記プログラムが前記ファイルに対してアクセスする際のアクセス属性と、を対応付けて記述されていることを特徴とする請求項１に記載のアクセス制御機能付き記憶装置。

【請求項３】　第２のアクセス制御手段が、
第１の属性情報及び第２の属性情報に変更を施すことのできる属性変更手段を有することを特徴とする請求項２に記載のアクセス制御機能付き記憶装置。

【請求項４】　第１の属性情報又は／及び第２の属性情報として、
属性変更手段のみが設定可能な、ファイルに対する属性情報の変更可否に関する情報を含むことを特徴とする請求項３に記載のアクセス制御機能付き記憶装置。

【請求項５】　第１の属性情報又は／及び第２の属性情報として、
属性変更手段のみが設定可能な、ファイルに対する追加書き込み可否に関する情報を含むことを特徴とする請求項３に記載のアクセス制御機能付き記憶装置。

【請求項６】　第１の属性情報として、
属性変更手段のみが設定可能な、ファイルに関する情報の取得可否に関する情報を含むことを特徴とする請求項３に記載のアクセス制御機能付き記憶装置。

【請求項７】　第１の属性情報又は／及び第２の属性情報として、
属性変更手段のみが設定可能な、ファイルに対する削除可否に関する情報を含むことを特徴とする請求項３に記載のアクセス制御機能付き記憶装置。

【請求項８】　プログラムの実行により、記憶手段に格納されているファイルへのアクセスが生じ、
第２の属性情報として、前記ファイルを示した第１の参照情報と前記プログラムを示した第２の参照情報との対応付けを示した情報が記述されていない場合、属性参照手段は、第１の属性情報を参照して、前記ファイルへのアクセス可否の判定を行うことを特徴とする請求項２に記載のアクセス制御機能付き記憶装置。

【請求項９】　プログラムの実行により、記憶手段に格納されているファイルへのアクセスが生じ、
前記アクセスが、第２の属性情報のアクセス属性の条件を満足していない場合、属性参照手段は、第１の属性情報を参照して、前記ファイルへのアクセス可否の判定を行うことを特徴とする請求項２に記載のアクセス制御機能付き記憶装置。

【請求項１０】　記憶手段全体又は一部である領域に対するアクセス属性情報である第３の属性情報を格納する手段を備え、
前記第３の属性情報として、前記領域に格納されたファイルに関する情報の取得可否に関する情報、又は／及び、前記領域内に属性変更可否に関する情報によって属性変更不可に設定されたファイルの存在有無を表す情報を含むことを特徴とする請求項４に記載のアクセス制御機能付き記憶装置。

【請求項１１】　１つ以上のファイルの集まりであるファイル群に対するアクセス属性情報である第４の属性情報を格納する手段を備え、
前記第４の属性情報として前記ファイル群に関する情報の取得可否に関する情報、又は／及び、前記ファイル群に対する属性変更可否に関する情報を含むことを特徴とする請求項４に記載のアクセス制御機能付き記憶装置。

【請求項１２】　第１の属性情報又は／及び第２の属性情報として、その属性の適用範囲に関する情報を含み、
前記適用範囲に関する情報に基づき、ファイルの一部に対するアクセス制御を行うことを特徴とする請求項１に記載のアクセス制御機能付き記憶装置。

【請求項１３】　第２のアクセス制御手段が、暗号手段と復号手段とを備え、
前記暗号手段は、記憶手段の全体もしくは一部、又は、記憶手段に格納された１つ以上のファイル、に暗号化を施して、前記暗号化の結果得られた暗号化データを前記記憶手段に格納し、
前記復号手段は、前記記憶手段に格納された前記暗号化データに復号化を施して、前記復号化の結果得られたデータを前記記憶手段に格納することを特徴とする請求項１に記載のアクセス制御機能付き記憶装置。

【請求項１４】　ファイルへのアクセスを制御するためにコンピュータを、
ファイルと前記ファイルに固有のアクセス属性である第１の属性情報を格納する記憶手段、
前記第１の属性情報を参照して前記ファイルに対するアクセス制御を行う第１のアクセス制御手段、
前記記憶手段内部の前記ファイルに対する条件に応じた

アクセス属性を記述した第２の属性情報を格納する手段、
前記第２の属性情報を参照して前記ファイルに対するアクセス制御を行う第２のアクセス制御手段、として機能させるためのファイル・アクセス制御プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、格納されたデータに対するアクセス及びデータを格納するアクセスに対して、適切なアクセス制御を実現するメモリカード等の記憶装置に関するものである。

【０００２】

【従来の技術】従来のメモリカードは、端末を限定せずにメモリカードにデータを書き込んだり、読み出したりするものである。そのため、端末を限定してアクセス制御を行うことはできない。

【０００３】一方、従来のＩＣカードは、利用可能な端末や利用者を限定することでデータを保護するものである。そのため、限定されない端末による利用を想定していない。

【０００４】

【発明が解決しようとする課題】以上のような従来のデータ記憶媒体にあっては、例えば銀行業務等の場合において、電子通帳としてメモリカードを利用する場合に、従来の通帳と同様に利用することを想定するならば、書き込みは、認証を行った正規の銀行端末のみが行うことができ、読み出しは、利用者が所有する端末等の一般の端末で、認証を行わずにできる必要がある。

【０００５】また、利用者の端末を利用したメモリカードのアクセスにおいて、通帳データの改ざんや削除に対する防御が必要となる。

【０００６】上記利用法を実現するためには、メモリカードに端末を限定しない場合と、認証を行って端末を限定する場合と、の両方に利用可能な機能を持たせることが必要である。また、端末を限定しない場合においても、読み出しのみ可能といった利用権限の限定を行う必要がある。

【０００７】本発明は、上記従来の要請に鑑みてなされたもので、上記のようなアクセス制御をメモリカード自体に行わせることによって、不正なファイルの削除や改ざんを防止することを目的とする。

【０００８】

【課題を解決するための手段】上記課題を解決するために、本発明は、第１に、ファイル固有のアクセス属性である第１の属性情報とは別に、第２のアクセス制御手段が、前記第２のアクセス制御手段内部のプログラムによるファイルへのアクセスを制御する際に参照する第２の属性情報属性情報を持つアクセス制御機能つき記憶装置である。

【０００９】これにより、第２のアクセス制御手段内のプログラムに対して、ファイル固有のアクセス属性（第１の属性情報）のみによる固定的・画一的・一括/包括的なアクセス制御とは異なる、特別な権限を与え、動的で多様なファイル・アクセス制御を実現することができる。

【００１０】本発明は、第２に、第１の属性情報又は／及び第２のアクセス属性情報として、第２のアクセス制御手段内の属性変更手段のみが設定可能な、ファイルの属性変更可否フラグ、ファイル情報の取得可否フラグ、追加書き込み可否フラグを備える。上記３種の属性フラグは、第１のアクセス制御手段経由では設定又は変更ができない。その他のフラグに関しても、属性変更可否フラグによって変更不可に設定されていれば、第１のアクセス制御手段経由での変更ができない。

【００１１】これにより、第２のアクセス制御手段経由で作成した重要なファイルに対する第１のアクセス制御手段経由でのアクセスを制限することができる。

【００１２】一方、第１のアクセス制御手段経由で作成したファイルのアクセス属性は、属性変更可否フラグ、情報取得可否フラグ、追加書き込み可否フラグを除いて、第１のアクセス制御手段経由で自由に変更することができる。

【００１３】本発明は、第３に、記憶手段の全体または一部に対して設定するアクセス属性情報と、記憶手段内部に属性変更不可に設定されたファイルの存在有無を表すフラグを備える。

【００１４】これにより、第１のアクセス制御手段経由での記憶手段に対するアクセスを制限することができ、第２アクセス制御手段経由でのみ利用可能な状態にすることができる。また、属性変更不可であるファイルが存在するときに、記憶手段全体に対する処理を拒否することで、属性変更不可であるファイルを守ることができる。

【００１５】本発明は、第４に、第１の属性情報が、属性適用範囲も同時に持ち、ファイルの一部に対するアクセス制御を行う。

【００１６】これにより、条件によって、アクセス可能な範囲を第２アクセス制御手段によって変化させることができる。

【００１７】

【発明の実施の形態】以下、本発明の実施の形態について、図１から図１２を用いて説明する。なお、本発明はこれら実施の形態に何等限定されるものではなく、その要旨を逸脱しない範囲において種々なる態様で実施し得る。

【００１８】図１は、本実施の形態の構成図である。図１において、１０１及び１０２は、端末と通信を行うインターフェースである。１０３は、端末が第１インターフェースを経由してフラッシュメモリにアクセスする場合に、ファイルシステム全体に対するアクセス属性及び

ファイルに付加されたアクセス属性を用いてアクセス制御を行うコントローラである。コントローラ１０３は、端末からのアクセス要求があった時に、ファイルシステムのアクセス属性及び対象ファイルのアクセス属性を参照し、アクセス要求がアクセス属性を満足していれば、アクセスを許可する。満足していなければアクセスを拒否する。ここでいう「アクセス」とは、ファイルに対する読み出し、書き込み、ファイルの情報取得、ファイルのアクセス属性変更であり、またそれ以外に考えられるすべてのファイルに対する操作である。

【００１９】１０４は、端末が第２インターフェースを経由してフラッシュメモリにアクセスする場合に、端末との間で認証を行い、認証結果に基づいてアクセス制御を行うセキュアチップである。本実施の形態では、セキュアチップ１０４は、内部に１つ以上のアプリケーションを保持し、認証状態によって起動されるアプリケーションが異なる。例えば、電子通帳ファイルに記帳を行うアプリケーションは、銀行端末が正規認証を行った場合のみ起動することができる。銀行端末でない場合、通帳記帳アプリケーションが起動されることはない。１０５はコントローラおよびセキュアチップからフラッシュメモリにアクセスするためのフラッシュインターフェース、１０６はフラッシュメモリである。

【００２０】コントローラ１０３の内部について図７を用いて説明する。コントローラ１０３は、内部に属性参照手段７０１とデータ通信路７０２を持つ。端末からあるファイルへのアクセス要求があると、属性参照手段７０１が対象ファイルのアクセス属性をチェックし、アクセス要求がアクセス属性を満足しているか判断する。満足していればデータ通信路７０２の利用が可能となり、アクセス要求を処理する。満足していなければ拒否する。

【００２１】セキュアチップ１０４の内部について図６を用いて説明する。セキュアチップ１０４は、認証手段６０１、アプリケーション群６０２、属性参照手段６０３、アプリケーションアクセス属性情報（属性テーブル）６０４、属性変更手段６０５を持つ。認証を行うための必要な情報を秘密に保持するために、セキュアチップ１０４は耐タンパとなっており、認証機能には、署名検証、乱数生成や暗復号化等の演算機能を含む。アプリケーションアクセス属性情報６０４は、起動されたアプリケーションによって、ファイルへのアクセス権限を変化させるためのものであり、ファイルに対応したアクセス権限を保持するアプリケーションと、そのアクセス属性が登録されている。第１インターフェース経由のアクセスよりも高い権限を与えるためのものである。アプリケーションアクセス属性情報６０４は、属性参照機能６０３によって参照され、属性変更機能６０５によって変更される。

【００２２】以下、図２を用いて、ファイルシステム及びファイルに付加されたアクセス属性について説明する。図２は、フラッシュメモリ上のファイルシステムの構成図の一例であり、２０１は、コントローラ経由でのアクセスに適用されるファイルシステム全体に対するアクセス属性の設定であり、Ｒは読み出し属性、Ｗは書き込み属性、Ｖはファイル情報取得属性（ファイル情報については後述）、Ｅはアクセス属性変更不可データの有無を表す。Ｒ、Ｗ、Ｖについては、０ならば不可、１ならば可を意味する。Ｅについては、０ならばアクセス属性変更不可データは存在せず、１ならば存在することを意味する。

【００２３】２０２は、コントローラ経由でのアクセスに適用されるファイルシステム内のファイル固有のアクセス属性であり、Ｒ、Ｗ、Ｖについてはファイルシステム全体のアクセス属性と同様なので説明を省略する。Ａは追記属性を意味する。Ｃについては、コントローラ経由によるアクセス属性変更可否を表す。１ならば変更可であり、０ならば変更不可を意味する。

【００２４】ファイル情報とは、ファイルの存在、ファイル名、ファイルサイズ、作成日時、アクセス属性であり、またそれ以外に考えられる全てのファイルに関する情報である。ファイル固有のアクセス属性２０２においてＶが０に設定されていると、コントローラ経由での対象ファイルに関する情報の取得が拒否される。また、ファイル一覧取得の要求に対してもＶが０に設定されているファイルは表示されない。

【００２５】ファイルシステム全体のアクセス属性２０１においてＶが０に設定されていると、ファイルシステム全体に対する情報の取得ができないので、結果として、コントローラ経由でのアクセスは全て拒否される。例えば、ファイルシステム全体のアクセス属性２０１において、ＲＷＶＥ＝１１１１、ファイル固有のアクセス属性２０２においてＲＷＡＣＶ＝１０００１に設定されているファイルの場合、フラッシュメモリ全体のアクセス属性がＶ＝１であるので、コントローラ経由で、ファイルに関する情報を取得することができる。また、Ｒ＝１であるので、ファイルの内容を読み出すことが出来る。しかしコントローラ経由での書きこみ要求に関しては、Ｗ＝０であるので、コントローラ１０３によって拒否される。もしＲＷＡＣＶ＝１０１０１のようにＷ＝０つまり書込み禁止設定であってもＡ＝１ならば、該当ファイルに対して、追記のみ可能である。

【００２６】また、アクセス属性の変更要求、例えばＲＷＡＣＶ＝１０００１から１１００１への変更要求を行ったとしても、Ｃ＝０より、コントローラ経由によるアクセス属性の変更は不可であるので、拒否される。Ｃ＝０であるファイルは、コントローラ経由によるファイルのアクセス属性変更が拒否される。また、ファイル名の変更、ファイルの削除を行うことが出来ない。現在の属性情報が対応するファイルの名称変更や属性情報自体の

消去は、属性情報変更とみなすからである。Ｃの変更が可能なのは、セキュアチップによる認証で、属性変更権限があるとみなされたアプリケーションによるアクセスのみであり、コントローラを経由したアクセスでは変更できない。

【００２７】別の例として、ファイルシステム全体のアクセス属性２０１において、ＲＷＶＥ＝１１１１、ファイル固有のアクセス属性２０２においてＲＷＡＣＶ＝１０１１１の場合，Ｗ＝０であるので、コントローラ経由での書きこみ要求に対しては、コントローラによって拒否されるが、Ｃ＝１よりアクセス属性の変更を行うことができるので、Ｗ＝１に変更することで、書き込みが可能となる。これによって、既存のメモリカードのように認証を介さない利用法も可能である。ファイルシステム全体のアクセス属性２０１に含まれるアクセス属性変更不可データの有無を表すＥが１である場合は、ファイルシステム全体に対する処理であるフォーマット等のコマンドを拒否することで、属性変更不可データを守ることができる（なお、ファイル情報のうち、ファイル名、ファイルサイズ等の情報の格納方法については、ここでは省略する）。

【００２８】以下、図３を用いて、アプリケーションアクセス属性情報６０４（３００）について説明する。図３は、セキュアチップ内部のアプリケーションアクセス属性情報の一例であり、３０１はフラッシュメモリ内のファイル１を表すファイル番号、３０２は、セキュアチップ内部のアプリケーション１を表すアプリケーション番号、３０３は、アプリケーション１がファイル１にアクセスする場合の、アクセス属性を表す。アクセス属性３０３の各項目ＲＷＡＣについては、ファイル固有のアクセス属性２０２で説明した項目と意味が同じであるので、説明を省略する。

【００２９】なお、アプリケーションアクセス属性は、１つのファイルに対して１つのアプリケーションのみを対応づけてもよいし、複数のアプリケーションを対応付けてもよい。その際、１つのファイルに対応したアプリケーションごとに異なるアクセス属性を設定してもよい。以下、端末からのフラッシュメモリへのアクセスについて説明する。図４は、コントローラを経由したフラッシュメモリへのアクセス処理の流れを示すフローチャートであり、図５はセキュアチップを経由したフラッシュメモリへのアクセス処理の流れを示すフローチャートである。図１乃至３とあわせてその流れを説明する。

【００３０】まずコントローラ経由のアクセスについては、端末にカードが挿入され（ステップ４０１）、端末は第１インターフェース１０１に対して、アクセス要求を行う（ステップ４０２）。コントローラ１０３内部の属性参照機能７０１は、まずフラッシュメモリ全体のアクセス属性２０１を参照し（ステップ４０３）、端末の要求と比較して（ステップ４０４）、アクセス属性を満足していなければ、コントローラ１０３がアクセス拒否を端末に伝える（ステップ４０５）。

【００３１】アクセス属性を満足している場合は、対象ファイルが存在している場合、属性参照機能７０１が対象ファイル固有のアクセス属性２０２を参照し（ステップ４０６）、端末の要求と比較する（ステップ４０７）。その後、アクセス属性を満足していなければ、コントローラ１０３が、端末にアクセス拒否を伝える（ステップ４０８）。一方、アクセス属性を満足していれば要求を処理する（ステップ４０９）。対象ファイルが存在していない場合は、アクセス要求がファイルの新規作成以外の場合はエラーを返し、ファイルの新規作成ならば処理（ファイル新規作成）を行う。

【００３２】次にセキュアチップ１０２経由のアクセスについては、端末にカードが挿入され（ステップ５０１）、端末とセキュアチップ１０４の間で認証を行う（ステップ５０２）。認証が完了すると、セキュアチップ１０４内部で認証結果に応じてアプリケーション群６０２の中から選択されたアプリケーションが起動される（ステップ５０３）。アプリケーションがファイルにアクセスを試みた時に（ステップ５０４）、ファイルが存在すれば、セキュアチップ１０４内部の属性参照機能６０３は、アプリケーションアクセス属性情報６０４を参照し（ステップ５０５）、該当ファイルにそのアプリケーションのアクセス属性が登録されているかどうかを調べる。そして、該当ファイルにそのアプリケーションのアクセス属性が登録されていれば、アプリケーションによるアクセスが、そのアクセス属性を満足しているかどうかを調べ（ステップ５０６）、アクセス属性を満足していれば、アプリケーションによるファイルへのアクセスを許可する（ステップ５０８）。

【００３３】アプリケーションアクセス属性情報６０４にアクセス属性が登録されていなかった場合、もしくは、登録されていたが、アクセス属性を満足しなかった場合は、フラッシュメモリ内部の対象ファイルが持つ、ファイル固有アクセス属性を参照し、これに従ってアクセスの可否を判定する（ステップ５０７）。

【００３４】ファイルが存在しなかった場合、アクセス要求が、ファイルの新規作成だった場合は、処理（ファイル新規作成）を行い、アプリケーションアクセス属性情報及びファイル固有アクセス属性は、ファイルを作成したアプリケーションによって指定され、属性変更機能６０５が設定する。

【００３５】ここで、属性参照手段によるアクセス可否判定のパターンをまとめると次のようになる。つまり、（１）第１の参照情報と第２の参照情報との対応付けが記述されていない場合と、（２）アクセス属性を満たさない場合（第１の参照情報と第２の参照情報との対応付けが記述されていてもアクセス属性が条件を満足しない場合）と、があり、（１）は、具体的には、プログラム

Ａの実行によりファイルＢへのアクセスが必要となった時に、(1-1)第１の参照情報として「ファイルＢ」の記述がない場合と、(1-2) 第２の参照情報として「プログラムＡ」の記述がない場合と、(1-3)それぞれに記述があっても、それらが対応付けされていない場合と、があり、そのような場合、属性参照手段は、第１の属性情報を参照して、ファイルＢへのアクセス制御を行う。

【００３６】電子通帳への書き込みや、電子チケットの新規作成、削除という処理を行うことができるのは、認証を経た銀行端末や、チケット販売端末といった特定の端末である必要がある。しかし、電子通帳、電子チケットの閲覧、表示を行う時には、認証によって端末を限定しない方が、処理時間や利用者の入力手間を考えると、便利である場合がある。

【００３７】本発明では、認証機能を持たない端末または認証を行っていない端末でも、ファイルに読み出し可能属性が与えられていれば、読むことができる。同時に、書き込み不可設定及びアクセス属性変更不可設定を行えば、認証機能を持たない端末から重要なファイルを変更される恐れがなく、安全かつ適切なセキュリティレベルを設定できるという効果がある。また、ファイルシステム全体のアクセス属性を変更できるセキュアチップ内のアプリケーションを利用すれば、認証を行った時のみファイルシステムを参照することが出来る、という機能を追加できる。

【００３８】これにより、メモリカードを郵送する場合にあらかじめコントローラ経由によるファイルシステムへのアクセスを全て禁止しておけば、もしメモリカード自体を盗まれたとしても第三者にファイルを読まれることを防止できる。解除する時は、セキュアチップによる認証を行い、セキュアチップ内のアクセス属性変更用アプリケーションを利用すれば、解除することが出来る。

【００３９】また、メモリカード内の情報を他人に見せたいが、変更、書き込み、削除といった処理を一切されたくない場合は、ファイルシステム全体のアクセス属性２０１において、ＲとＶを１に設定し、Ｗを０に設定すれば、セキュアチップによる認証を行ってファイルシステムのアクセス属性を変更しない限り、読み出し専用メモリカードとなる。

【００４０】さらに、図９のように、属性変更手段６０５によるコントローラ経由によるファイルシステムへのアクセスの禁止と同時に、暗号化手段９０１を用いてセキュアチップのみが秘密に保持する暗号鍵９０２によってファイルシステム内のファイルに暗号化を施すことによって、例えメモリカードを分解してフラッシュメモリの内容を特殊な方法で直接読まれたとしても、容易には内容を読み出せないようにすることができる。

【００４１】解除する時は、図１０のように、属性変更手段６０５によるファイルシステムへのアクセスの許可と同時に、復号化手段１００１を用いてセキュアチップのみが秘密に保持する復号鍵１００２で暗号化データを復号化してファイルを復元する。この暗復号処理の実行を、ファイルシステム全体のアクセス属性変更権限の持つアプリケーションのみに限定しておけば、認証を伴わずに容易にフラッシュメモリ内のデータを読み出すことは困難となる。

【００４２】なお、ファイルは、フラッシュメモリのアドレス直接指定による特定範囲であってもよい。また、ファイル固有のアクセス属性は、ファイルの一部に対するアクセス属性であってもよい。その場合、アクセス属性を設定する範囲を表すための情報をアクセス属性に含める。例えば、図８のように、ファイル先頭からの位置を表すｓと、アクセス属性を設定するサイズｅをアクセス属性に含めるといった具合である。また、例えば、格納データとして音楽ファイルを扱う場合に、料金未納時は音楽ファイルの先頭一部のみ読み出し可能に設定し、料金を支払うと、セキュアチップによって音楽ファイル全体を読み出し可能に設定するなどにより、視聴機能を実現できる。

【００４３】また、アプリケーションは、ハードウェア（のみ）で構成された回路でもよい。また、ファイル固有の属性情報または、アプリケーションアクセス属性情報として、ファイルの削除の可否を表すフラグを属性変更可否フラグとは別に独立して持ってもよい。

【００４４】また、メモリカードの構成は、図１１のようにひとつのインターフェースを介して端末と通信し、セキュアチップに対する要求はコントローラを経由してセキュアチップに送信される構成でもよい。

【００４５】また、メモリカードの構成は、図１２のようにひとつのインターフェースを介して端末と通信し、通信内容によってコントローラとセキュアチップにデータが振り分けられる構成でもよい。

【００４６】また、アプリケーションアクセス属性情報は、セキュアチップによってのみアクセス可能であれば、セキュアチップの外に設置してもよい。

【００４７】また、端末によるフラッシュメモリへのアクセスは、コントローラ及びセキュアチップとの通信路とは別に、データ転送用の通信路を持ち、コントローラ及びセキュアチップによって、そのデータ通信路を制御してもよい。

【００４８】また、本実施の形態におけるフラッシュメモリは、コントローラおよびセキュアチップによって制御可能であり、かつコントローラおよびセキュアチップを経由しなければアクセスが出来ないその他の記録媒体でもよい。

【００４９】また、アクセス属性について、ＶとＣの２つを、両者ともに０ならば、ファイル情報取得不可、Ｖのみ０であれば従来のフラッシュメモリにおける隠しファイル、Ｃのみ０であればアクセス属性変更不可、両者のみ１であれば、ファイル情報取得及びアクセス属性変

更に関して制限なし、というように相関させてもよい。

【００５０】

【発明の効果】以上説明したように、本発明によれば、セキュアチップによって作成されたファイルのうち、アクセス属性変更を不可に設定したファイルは、コントローラ経由のアクセスでは、属性を参照するのみで変更することが出来ない。しかし、セキュアチップによって端末を認証し、正規のアクセス権限を持つアプリケーションによってのみ属性を変更することができる。これにより、従来のメモリカードでは行うことができなかった、メモリカード自身によるアクセス制御が可能になるという効果がある。

【００５１】また、コントローラ経由では見られたくない重要なファイルのファイル情報取得属性を、セキュアチップによって不可に設定することで、コントローラ経由ではそのファイルの存在自体を知ることができなくなり、ファイルに対する不正の機会を減らすことが出来る。一方、コントローラを経由して作成されたファイルに関しては、アクセス属性は自由に設定することができ、従来のメモリカードと同じアクセス属性の設定も可能であるという効果がある。

【００５２】また、ファイルシステム全体のアクセス属性を変更して、コントローラからのアクセスを完全に禁止することで、メモリカードを輸送するときや他人に預けるときに、第三者によるフラッシュメモリへのアクセスを禁止することや、読み出し専用に設定できるという効果がある。

【図面の簡単な説明】

【図１】本発明の実施の形態におけるメモリカード構成図

【図２】本発明の実施の形態におけるファイルに固有のアクセス属性情報の図

【図３】本発明の実施の形態におけるセキュアチップ内部のアプリケーション別アクセス属性テーブルの図

【図４】本発明の実施の形態におけるコントローラ経由による端末からのアクセスのフローチャート

【図５】本発明の実施の形態におけるセキュアチップ経由による端末からのアクセスのフローチャート

【図６】本発明の実施の形態におけるセキュアチップ内部の構成図

【図７】本発明の実施の形態におけるコントローラ内部の構成図

【図８】本発明の実施の形態におけるファイルの一部に適用されるアクセス属性情報の図

【図９】本発明の実施の形態における暗号化機能をもったセキュアチップ内部の構成図

【図１０】本発明の実施の形態における復号化機能を持ったセキュアチップ内部の構成図

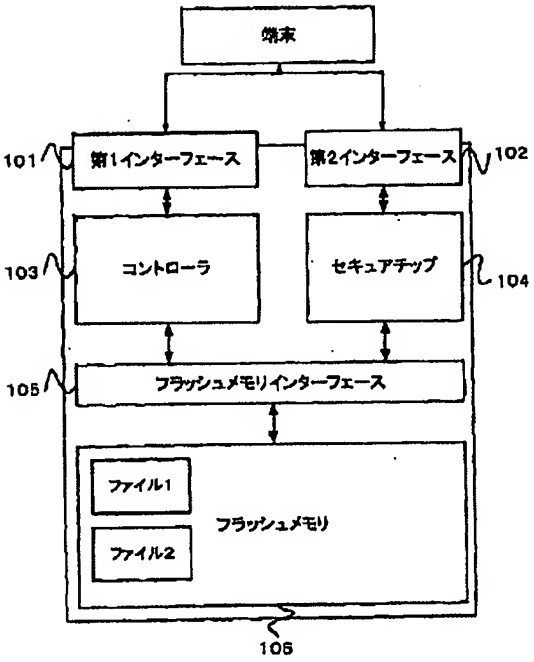
【図１１】本発明の実施の形態におけるインターフェースが１つであり、端末のセキュアチップとの通信はコントローラ経由で行うメモリカード構成図

【図１２】本発明の実施の形態におけるインターフェースが１つであり、通信内容によってコントローラとセキュアチップにデータが振り分けられるメモリカード構成図

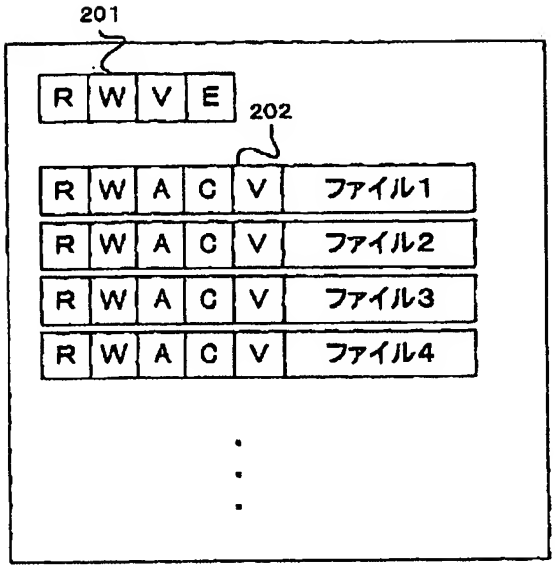
【符号の説明】

１０１　第１インターフェース
１０２　第２インターフェース
１０３、１１０３、１２０３　コントローラ
１０４、１１０４、１２０４　セキュアチップ
１０５　フラッシュメモリインターフェース
１０６　フラッシュメモリ
２０１　ファイルシステム全体のアクセス属性
２０２、８０１　ファイルに固有のアクセス属性
３００　アクセス属性テーブル
３０１　ファイル番号
３０２　アプリケーション番号
３０３　アプリケーションに対応したアクセス属性
６０１　認証手段
６０２　アプリケーション群
６０３、７０１　属性参照手段
６０４　アプリケーション別アクセス属性テーブル
６０５　属性変更手段
６０６、７０２　データ通信路
９０１　暗号化手段
９０２　暗号鍵
１００１　復号化手段
１００２　復号鍵
１１０１、１２０１　インターフェース

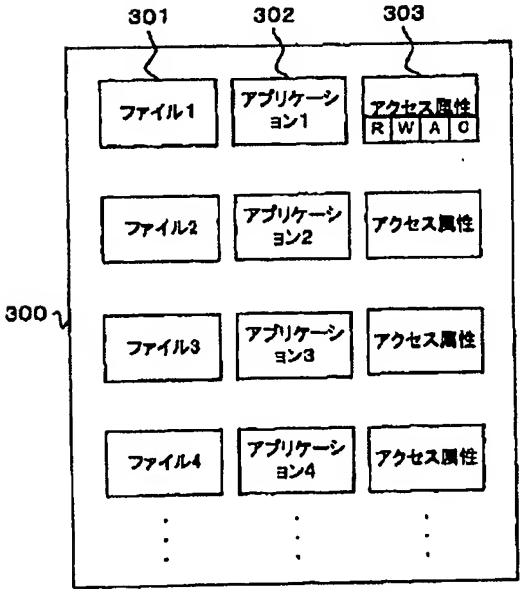
【図1】


端末
第1インターフェース
第2インターフェース
101
102
コントローラ
セキュアチップ
103
104
フラッシュメモリインターフェース
105
ファイル1
ファイル2
フラッシュメモリ
105

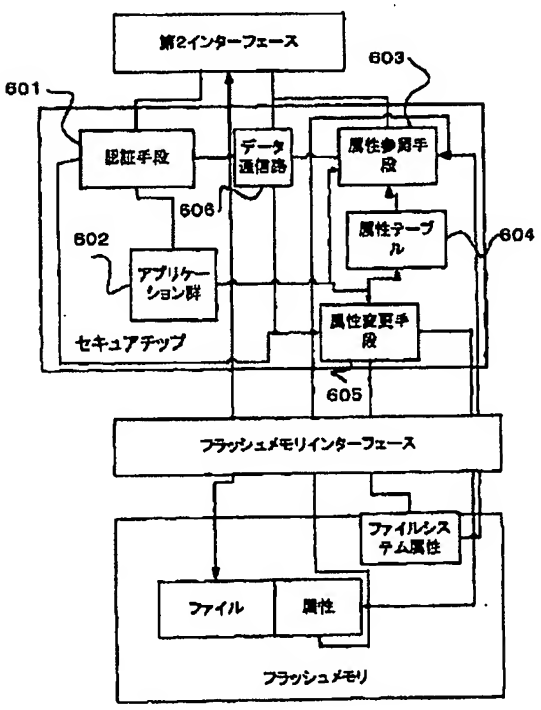
【図2】


201
R W V E
202
R W A C V ファイル1
R W A C V ファイル2
R W A C V ファイル3
R W A C V ファイル4

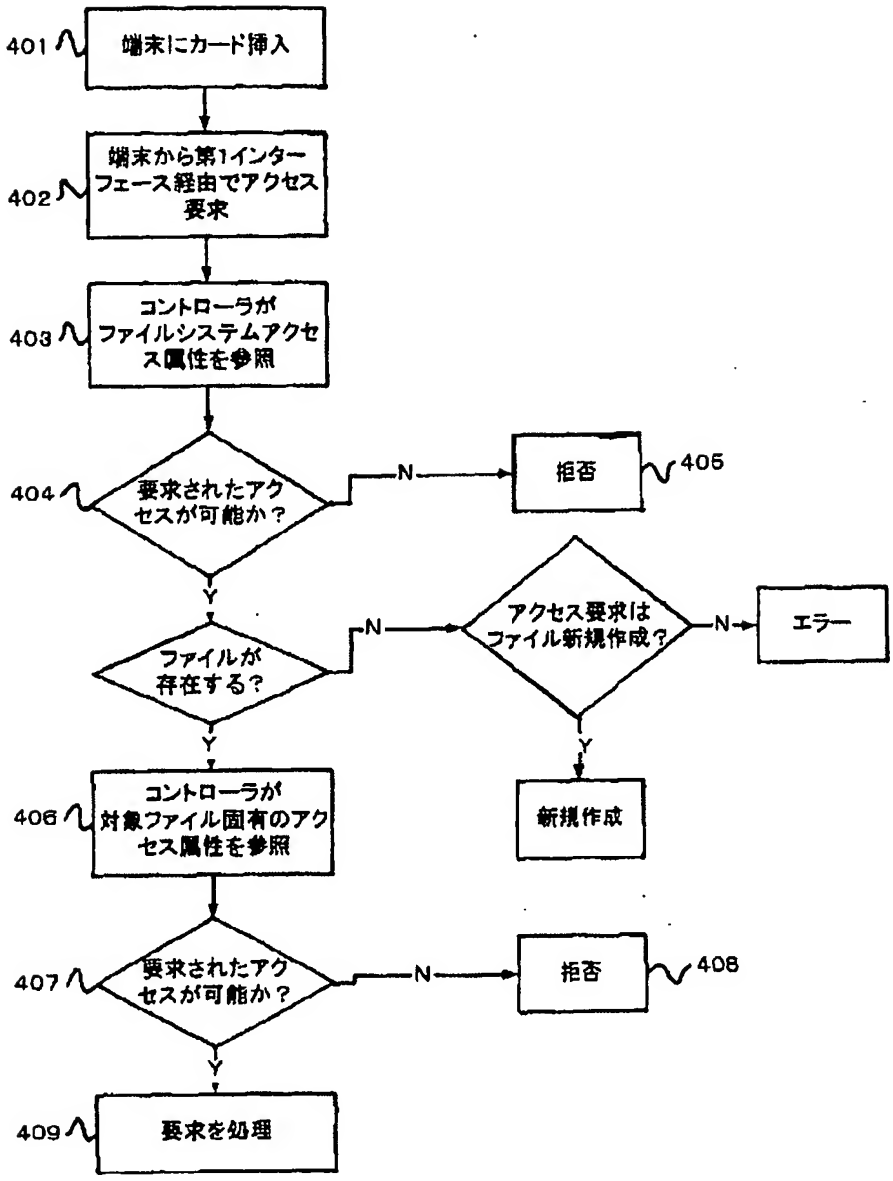
【図3】


301
302
303
ファイル1
アプリケーション1
アクセス属性
R W A C
ファイル2
アプリケーション2
アクセス属性
300
ファイル3
アプリケーション3
アクセス属性
ファイル4
アプリケーション4
アクセス属性

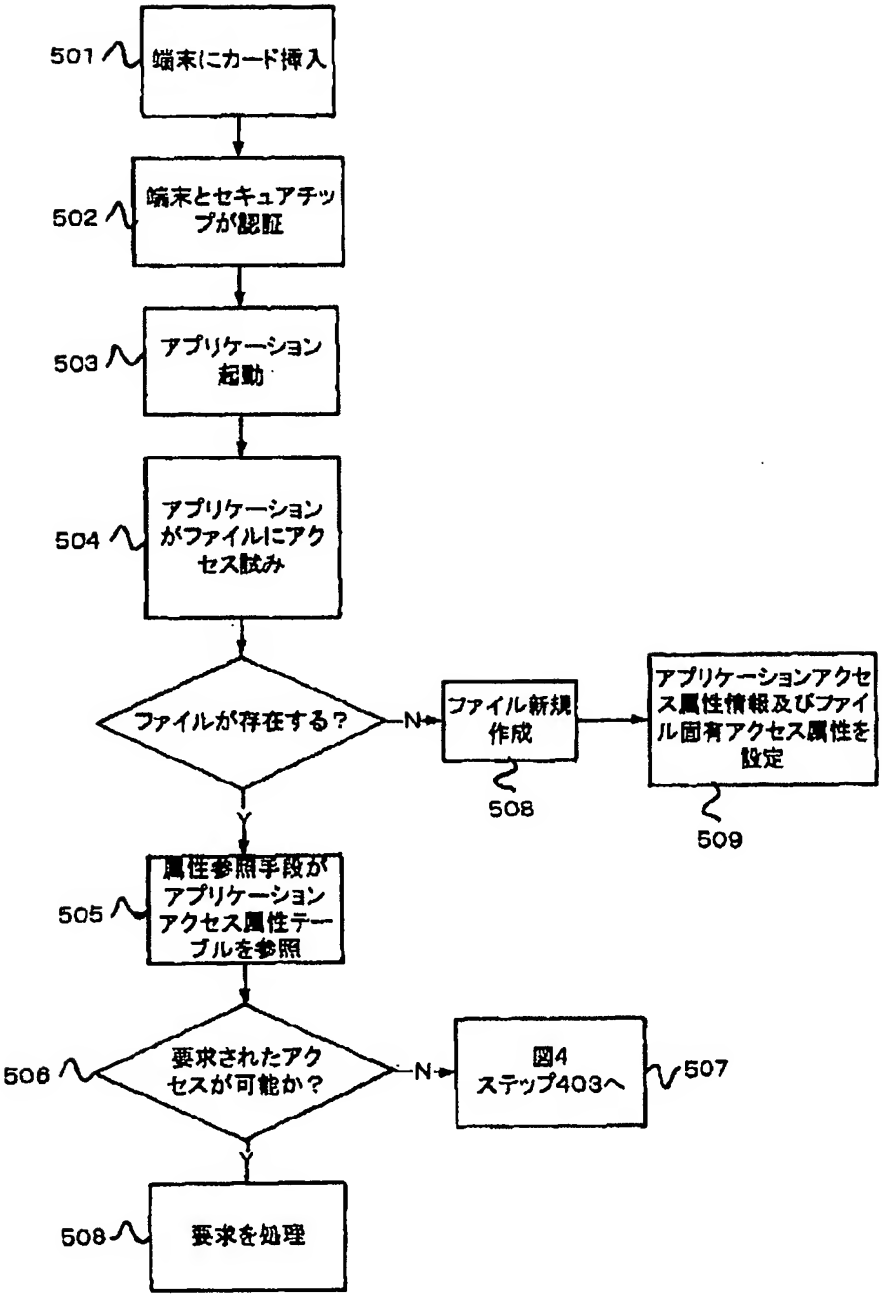
【図6】


第2インターフェース
601
603
認証手段
データ通信路
属性参照手段
606
602
属性テーブル
604
アプリケーション群
セキュアチップ
属性変更手段
605
フラッシュメモリインターフェース
ファイルシステム属性
ファイル
属性
フラッシュメモリ

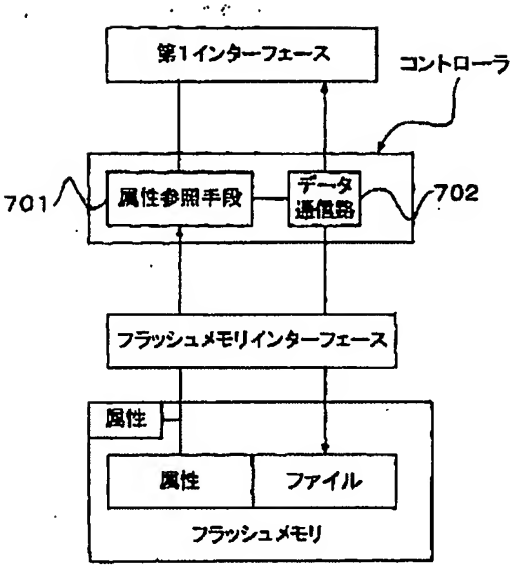
【図４】


401
端末にカード挿入
402
端末から第1インターフェース経由でアクセス要求
403
コントローラがファイルシステムアクセス属性を参照
404
要求されたアクセスが可能か？
N
405
拒否
Y
ファイルが存在する？
N
アクセス要求はファイル新規作成？
N
エラー
Y
Y
406
コントローラが対象ファイル固有のアクセス属性を参照
新規作成
407
要求されたアクセスが可能か？
N
408
拒否
Y
409
要求を処理

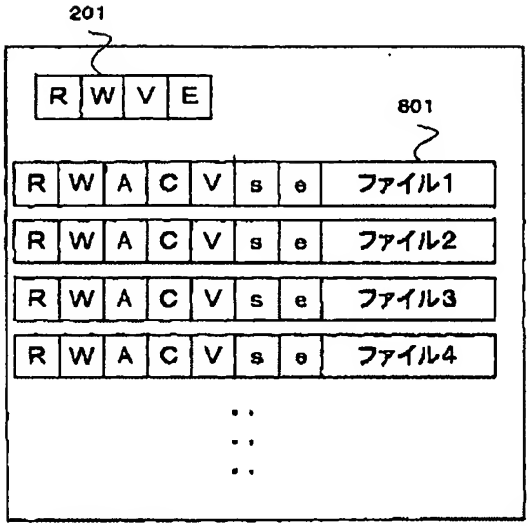
【図５】


501
端末にカード挿入
502
端末とセキュアチップが認証
503
アプリケーション起動
504
アプリケーションがファイルにアクセス試み
ファイルが存在する？
N
ファイル新規作成
508
アプリケーションアクセス属性情報及びファイル固有アクセス属性を設定
509
Y
505
属性参照手段がアプリケーションアクセス属性テーブルを参照
506
要求されたアクセスが可能か？
N
図4 ステップ403へ
507
Y
508
要求を処理

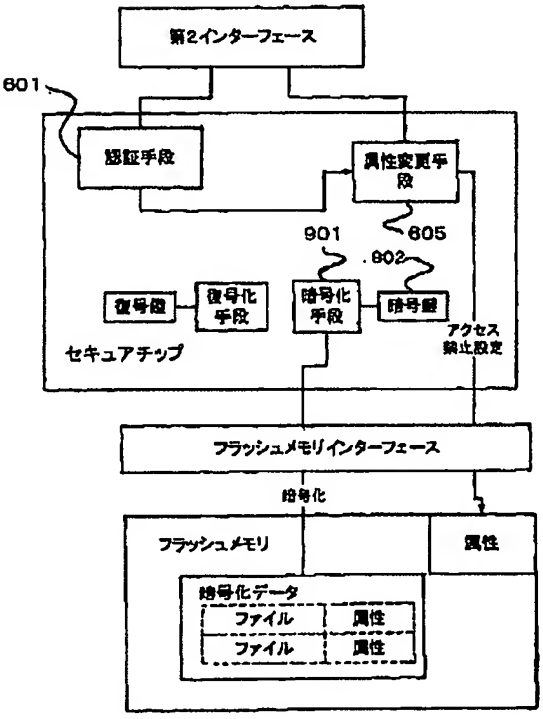
【図7】


第1インターフェース
コントローラ
701
属性参照手段
データ通信路
702
フラッシュメモリインターフェース
属性
属性
ファイル
フラッシュメモリ

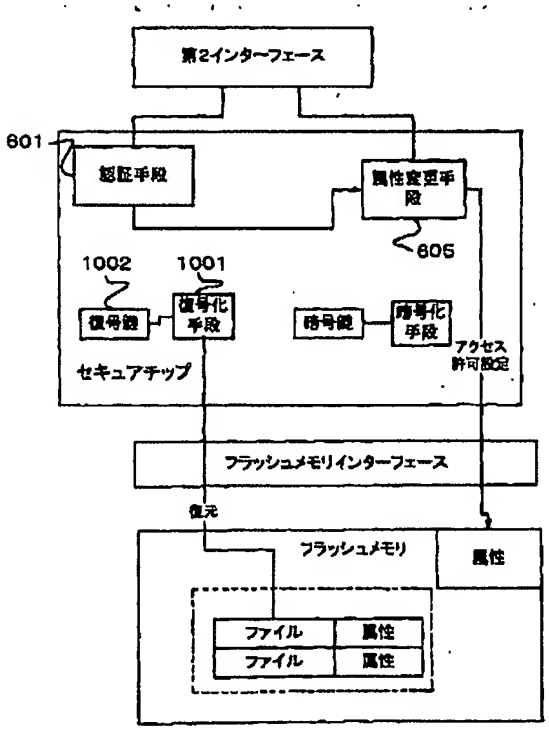
【図8】


201
R W V E
801
R W A C V s e ファイル1
R W A C V s e ファイル2
R W A C V s e ファイル3
R W A C V s e ファイル4

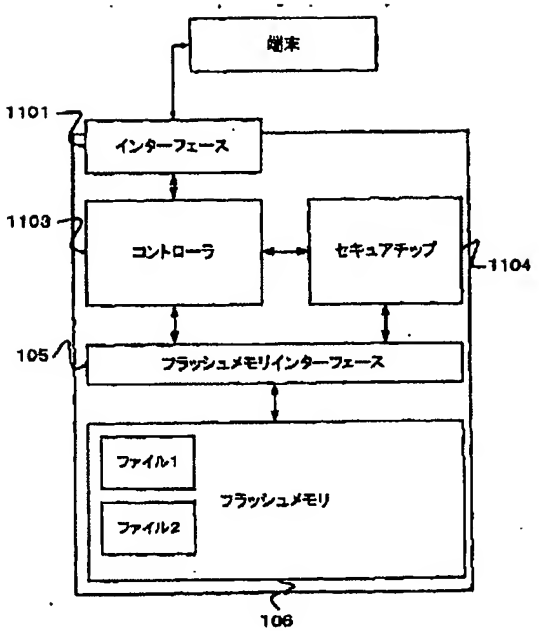
【図9】


第2インターフェース
601
認証手段
属性変更手段
605
901
902
復号鍵
復号化手段
暗号化手段
暗号鍵
アクセス禁止設定
セキュアチップ
フラッシュメモリインターフェース
暗号化
フラッシュメモリ
属性
暗号化データ
ファイル
属性
ファイル
属性

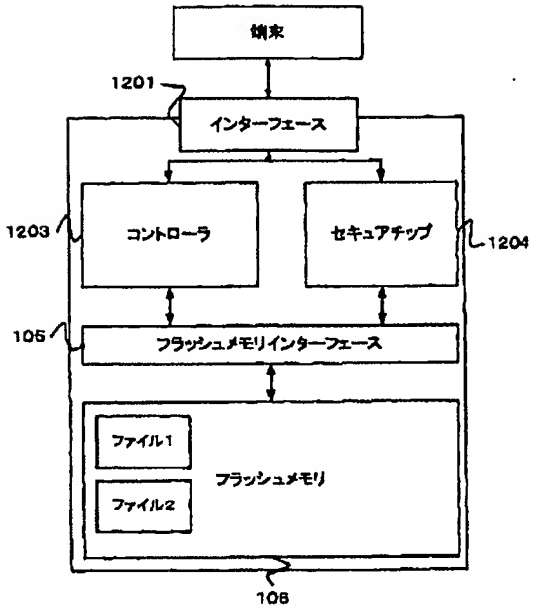
【図10】


第2インターフェース
601
認証手段
属性変更手段
605
1002
1001
復号鍵
復号化手段
暗号鍵
暗号化手段
アクセス許可設定
セキュアチップ
フラッシュメモリインターフェース
復元
フラッシュメモリ
属性
ファイル
属性
ファイル
属性

【図１１】



【図１２】



フロントページの続き

(72)発明者　佐々木　理
大阪府門真市大字門真1006番地　松下電器
産業株式会社内

Ｆターム(参考)　5B017 AA07 BA06 BB06 CA16
5B035 AA13 BB09 CA38
5B082 EA11 JA06